IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF: IPHONE 6 CELL PHONE WITH BLACK CASE AND CRACKED SCREEN; Evidence Log Number 20-024, Item #1 CURRENTLY LOCATED AT THE BROOKVILLE POLICE DEPARTMENT EVIDENCE ROOM AT 70 SECOND STREET, SUITE B, BROOKVILLE, PA 15825.	Magistrate No. 3:21-12 MJ **[UNDER SEAL]**

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

INTRODUCTION AND AGENT BACKGROUND

I, Craig M. NEEDHAM, being duly sworn, depose and state:

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Pennsylvania State Trooper currently assigned to the Pennsylvania State Police Troop C Vice Unit and have been so for 12 years. I have been sworn as a Task Force Officer with the Drug Enforcement Administration for approximately one year.

3. In my capacity as a Pennsylvania State Trooper and a Task Force Officer with DEA, I have been involved in numerous federal and/or state search warrants/investigations and have subsequently arrested and/or directly assisted in the arrests of drug law violators. In the course of my training and experience, I have become familiar with the methods and techniques associated with the

distribution of narcotics, the laundering of drug proceeds, and the organization of drug conspiracies. In the course of conducting these investigations, I have been involved in the use of the following investigative techniques: interviewing informants and cooperating witnesses, conducting physical surveillance, and being trained in: consensual monitoring and recording of both telephonic and non-telephonic communications, analyzing pen register data, conducting court-authorized wire and oral interception electronic surveillance. I have also prepared and executed search warrants, which have led to substantial seizures of narcotics, firearms, contraband, and evidence of criminal activity.

4. Further, based on my training and experience, I am aware that it is common practice for drug traffickers who desire to insulate themselves from detection by law enforcement to routinely utilize multiple telephones, counter surveillance, false or fictitious identities, and coded communications in order to communicate with their customers, suppliers, couriers, and co-conspirators. Moreover, it is not unusual for drug traffickers to initiate or subscribe such phone services in fictitious names or under the name of an associate or family member in an effort to thwart detection by law enforcement. Also, it is now a common practice for drug traffickers to utilize all communication features of their telephones, most notably the voice call and text message features, nearly simultaneously, to communicate with their conspirators and customers. For example, it is quite common for a particular transaction to be set up and completed using both voice calls and text messages. In fact, it is now quite unusual for a drug trafficker to utilize solely one feature of a telephone, such as the voice call feature, to further his criminal activities while not also using another feature, such as the text message feature, to further his criminal activities.

5. I am an "investigative or law enforcement officer of the United States" within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States, who is empowered by law to conduct investigations of, and make arrests for, controlled substance offenses enumerated in Title 21, United States Code.

6. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

RELEVANT CRIMINAL STATUTES

7. Under Title 21, United States Code, Sections 841(a)(1) and 841(b)(1)(A), it is unlawful for any person to knowingly, intentionally and unlawfully possess with intent to distribute and distribute methamphetamine and/or a quantity of a mixture and substance containing a detectable amount of methamphetamine, a Schedule II controlled substance.

8. Under Title 21, United States Code, Section 846, it is unlawful for any two or more persons to knowingly, intentionally and unlawfully conspire with one another to possess with intent to distribute and distribute methamphetamine and/or a quantity of a mixture and substance containing a detectable amount of methamphetamine, a Schedule II controlled substance, contrary to the provisions of Title 21, United States Code, Sections 841(a)(1) and 841(b)(1)(A).

IDENTIFICATION OF THE DEVICE(S) TO BE EXAMINED

9. The property to be searched is:

> IPHONE 6 CELL PHONE WITH BLACK CASE AND CRACKED SCREEN, with Evidence Log Number 20-024, Item #1.

Hereinafter the "Device". The Device is currently located at Brookville Police Department Evidence Room at 70 Second Street, Suite B, Brookville, PA 15825.

10. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

11. The Device is currently in the lawful possession of Brookville Police Department. The Device came into their possession on March 15, 2020 pursuant to the execution of a lawful search warrant on a 1998 tan Ford Explorer bearing PA registration LFL9187. Said vehicle was utilized by Dennis RAUCH when he was taken into custody and the vehicle seized during a drug investigation in

Brookville Borough on March 14, 2020. After RAUCH was taken into custody, he required transportation to Brookville Hospital after he admitted to ingesting Suboxone and Xanax and advised he was feeling ill. The subsequent execution of a lawful search warrant of the 1998 tan Ford Explorer was conducted in the secure custody of the BROOKVILLE Police Department on March 15, 2020. Pursuant to the execution of the search warrant investigators recovered the following items:

IPHONE 6 CELL PHONE WITH BLACK CASE AND CRACKED SCREEN, Evidence Log #20-024, Item #1

92.9 GRAMS OF METHAMPHETAMINE

RUGER P95 9MM HANDGUN

APPROXIMATELY 100 ROUNDS OF AMMUNITION

NUMEROUS ITEMS OF DRUG PARAPHERNALIA

12. At the time of the search incident on March 15, 2020, Dennis RAUCH had been identified as being related to the investigation of an extensive drug trafficking organization in the Western District of Pennsylvania. Pursuant to the execution of the search warrant, law enforcement officers seized the Device. Therefore, while the DEA might already have all necessary authority to examine the Device, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

13. The Device is currently in storage at Brookville Police Department Evidence Room at 70 Second Street, Suite B, Brookville, PA 15825. In my training and experience, I believe that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as it was when the Device first came into the possession of the Brookville Police Department.

FACTS AND CIRCUMSTANCES

14. Your Affiant is participating in a drug trafficking investigation of individuals identified as John BISBEE, Alexis BROLIN, Tammie BROLIN, Cassandra WALLACE, Davin GOWER, Jared NYMAN, Andrew KNEPP, Nicole GAINES, Jeffrey SWANSON, Brian GIDNEY, Dennis RAUCH, Brittany LUZIER and others, who are members of a multi-state drug trafficking organization, hereinafter the "Organization".

15. From November of 2019 through June of 2020, your Affiant participated in the monitoring and concurrent surveillance during Title III wiretaps of John BISBEE, Alexis BROLIN and Nicole GAINES. Each of the members of the Organization were identified as methamphetamine traffickers and the Organization was responsible for in excess of 20 kilograms of methamphetamine being distributed throughout the Western District of Pennsylvania.

16. As described above, on March 14, 2020, law enforcement members seized the 1998 Ford Explorer utilized by RAUCH during a drug investigation in Brookville, PA. When the vehicle was searched the following day, officers recovered the Device, methamphetamine and a firearm from the vehicle.

17. On June 3, 2020 an Indictment was filed at Case Number 3:20-07, and on August 4, 2020 a Superseding Indictment was filed at Case Number 3:20-07 charging John BISBEE, Alexis BROLIN, Tammie BROLIN, Cassandra WALLACE, Davin GOWER, Jared NYMAN, Andrew KNEPP, Nicole GAINES, Jeffrey SWANSON, Brian GIDNEY, Dennis RAUCH, Brittany LUZIER and others in the United States District Court for the Western District of Pennsylvania with multiple charges related to the drug trafficking, firearms violations and money laundering conspiracy.

18. Your Affiant knows that throughout the methamphetamine trafficking investigation that began in the summer of 2019 until June 9, 2020, Alexis BROLIN, Tammie BROLIN and other members of the Organization received methamphetamine from Nicole GAINES and Andrew KNEPP initially and then John BISBEE and others to redistribute throughout the Western District of Pennsylvania. Through Title III interceptions, physical surveillance and other methods, both Dennis RAUCH and his paramour Brittany LUZIER were intercepted, and later identified, in approximately 4 transactions as a redistributor for Alexis BROLIN between January 2, 2020 and April 2, 2020 involving multiple ounce weights of methamphetamine.

19. On June 9, 2020 an arrest warrant was issued for DENNIS RAUCH based on the Indictment and was later executed by U.S. Marshal Service who apprehended RAUCH and LUZIER in Mississippi on approximately August 7, 2020.

EVIDENCE COMMONLY STORED ON CELL PHONES AND OTHER ELECTRONIC STORAGE DEVICES

20. Based on my training and experience, as well as the collective knowledge and experience of other agents and officers associated with this investigation, I am aware that it is common practice for drug traffickers and their co-conspirators to routinely utilize cellular telephones to communicate with their customers, suppliers, couriers, and other conspirators for the purpose of insulating themselves from detection by law enforcement. Moreover, it is not unusual for them to initiate such mobile or prepaid phone service in the name of an associate or family member, or in the name of a fictitious individual. These individuals often require the use of cellular telephones to negotiate times, places, schemes, and manners for importing,

possessing, concealing, and distributing controlled substances, and for arranging the disposition of proceeds derived from the sale of controlled substances.

21. Evidence of drug, money laundering and firearm crimes can be found in the electronic storage within cellular telephones, electronic tablets, iPads, laptop computers, memory cards and flash drives. Such evidence can include internet searches for drug-related paraphernalia, addresses, telephone numbers and contacts, as well as incriminating photographs and communications via emails, text messages or instant messages. With the advance of technology, the distinction between computers and cellular telephones is quickly becoming less clear. Actions such as internet searching or emailing, in addition to calling and text messaging, can now be performed from many cellular telephones. In addition, those involved in drug trafficking crimes commonly communicate using multiple cellular telephones. I am also aware in some instances drug dealers will replace a cellular telephone and/or the cellular telephone number with varying frequency and maintain custody of the replaced cellular telephone for future use and/or reference. Contemporaneous possession of multiple cellular telephones may be evidence of drug trafficking. Moreover, the particular number of, and the particular numbers dialed by, particular cellular telephones may be evidence of drug trafficking, particularly in a case involving the interception of communications between drug traffickers. Such numbers can confirm the identities of particular speakers and the occurrence of certain events. As with most electronic/digital technology items, communications made from an electronic device, such as a cellular telephone, are often saved or stored on the device.

22. As with most electronic/digital technology items, communications made from an electronic device, such as a cellular telephone or a standard computer, are often saved or stored on the device. Storing this information can be intentional, for example, by saving a text message or a contact

or an e-mail. Digital information can also be retained unintentionally. Traces of the path of an electronic communication, an internet search, and the locations of photographs and videos may be automatically stored in many places on a computer or cellular telephone. In addition to electronic communications, a user's internet activities generally leave traces in the web cache and internet history files. A forensic examiner often can recover evidence that shows when and in what manner a user of an electronic device, such as a computer or a cell phone, used such a device.

23. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they often can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on an electronic storage device such as a computer, the data contained in the file often does not actually disappear; rather, that data often remains on the device until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space -- that is, in space on a device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space -- for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from an electronic storage device depends less on when the file was sent, downloaded, or viewed than on a particular user's operating system, storage capacity, and habits.

24. I am aware that those who illegally possess drugs sometimes take trophy photographs and videos using their cameras and/or cellular telephones of their drugs, firearms, and proceeds and retain them on those devices. In addition, I am aware that drug traffickers, like law-abiding citizens, sometimes take photographs and videos using their cameras and cellular telephones of themselves with their friends, relatives, and associates and keep the photographs and videos on those devices. When they are taken or retained by drug traffickers, such photographs and videos can be evidence, and can lead to additional evidence, of illegal trafficking activity by identifying the traffickers, contraband, and people who are actively assisting and/or supporting the trafficking activity as well as the locations where they live or where they store their drugs, firearms, proceeds, or paraphernalia.

25. It should be noted that data on electronic communication and/or storage devices is often relevant to a criminal investigation by revealing who used a particular device. In addition, such data can reveal who resided at or who had access to a particular location if, for example, a particular device was found at a particular location (e.g., inside a particular room of a particular residence) and the device contains data demonstrating that it was used by or belonged to a particular person. In that sense, a particular electronic device can be significant indicia linking a particular person to contraband or other criminal activity even if the device itself does not contain the remnants of incriminating communications.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

26. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

27. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because

special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

FORENSIC EVIDENCE: DELETED FILES, USER ATTRIBUTION

28. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the

device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device to traffic in illegal drugs, engage in money laundering or firearm offenses, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely

to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

29. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

30. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

31.. Based upon the forgoing, there is probable cause to conclude that included within the electronic device described will be evidence of violations of Title 21, United States Code, Sections 841(a)(1) (distribution and possession with intent to distribute controlled substances); and 846 (conspiracy to distribute and to possess with the intent to distribute controlled substances).

32. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B and I request that the Court issue the proposed search warrant.

33. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

The above information is true and correct to the best of my knowledge, information and belief.

/s/ Craig M. Needham
CRAIG M. NEEDHAM
Pennsylvania State Trooper
Task Force Officer, DEA

Sworn and subscribed before me by telephone
pursuant to Fed. R. Crim. P. 4.1(b)(2)(A)
this 7th day of January, 2021.

KEITH A. PESTO
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

PROPERTY TO BE SEARCHED

IPHONE 6 CELL PHONE WITH BLACK CASE AND CRACKED SCREEN, Evidence Log Number 20-024, Item #1

which is currently stored at the Brookville Police Department Evidence Room at 70 Second Street, Suite B, Brookville, PA 15825.

ATTACHMENT B

ITEMS TO BE SEARCHED FOR AND SEIZED

1. All records, information and items on the Devices described in Attachment A, including:

a. Contact lists, including telephone numbers and names associated with those numbers;

b. Incoming and outgoing call logs;

c. Incoming and outgoing text messages, including draft text messages;

d. Sent and received audio files;

e. Photographs and/or videos;

f. Emails and/or voice mails;

g. Navigation, mapping, and GPS files;

h. Online/social media postings;

i. Call forwarding information; and

j. Internet searches.

2. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form. However, no real-time communications will be intercepted and searched during service.